Simplifier les audits sur la sécurité et surveiller les activités des utilisateurs privilégiés au moyen d'un tableau de bord permettant de contrôler la conformité aux exigences de sécurité

Tivoli software

IBM Tivoli Compliance Insight Manager

Points forts

- Automatisation des rapports d'audit grâce à un tableau de bord permettant de contrôler la conformité et de générer, de manière flexible, la distribution de rapports
- Création de modules personnalisés de gestion de la conformité via des règles d'administration établies et des moteurs de définition de rapports
- Prise en charge des besoins d'audits en convertissant en langage simple les données enregistrées des logs d'audit natifs
- Collecte, stockage, étude et récupération des logs grâce à une gestion automatisée des logs
- Simplification de l'ajout de nouveaux collecteurs et analyseurs de logs grâce à un kit d'outils avancé
- Surveillance et audit performants des utilisateurs privilégiés (PUMA) sur les bases de données, les applications, les serveurs et les grands systèmes
- Intégration à IBM Tivoli Identity Manager, IBM Tivoli Access Manager et IBM Tivoli Security Operations Manager afin d'optimiser le travail entrepris pour assurer le respect de la conformité et traiter les incidents

Un grand nombre d'entreprises se trouve confronté au problème de gestion du nombre incalculable de données des logs qu'il faut conserver à des fins d'audit. Il leur faut tout d'abord regrouper de manière fiable et vérifiable les données provenant de sources dispersées dans l'entreprise, et ce de façon continue et viable. Après avoir collecté des milliards d'entrées de logs, il faut un moyen rapide et efficace d'en faire quelque chose.

Or, la collecte et l'analyse de telles informations peuvent prendre un temps considérable et demander une certaine expertise. Et bon nombre d'organisations – déjà limitées en ressources – n'ont simplement ni le temps ni la main-d'oeuvre pour cela. C'est pour cette raison qu'IBM Tivoli Compliance Insight Manager a été élaborée. Solution automatisée permettant de surveiller et d'analyser les activités des utilisateurs au sein de l'entreprise puis d'établir des rapports, Tivoli Compliance Insight Manager fournit la preuve écrite, non intrusive et en continu, que vos données et systèmes sont gérés conformément aux politiques de l'entreprise.

Saisir rapidement les activités des utilisateurs grâce à un tableau de bord complet

Tivoli Compliance Insight Manager offre un tableau de bord simple d'utilisation, permettant de surveiller la conformité aux exigences de sécurité et qui résume des milliards de fichiers logs dans une présentation graphique. Vous pouvez ainsi obtenir rapidement une vue d'ensemble de votre position par rapport aux exigences de sécurité, comparer les activités des utilisateurs et les événements liés à la sécurité à des systèmes de référence et surveiller ces événements ainsi que les utilisateurs privilégiés.

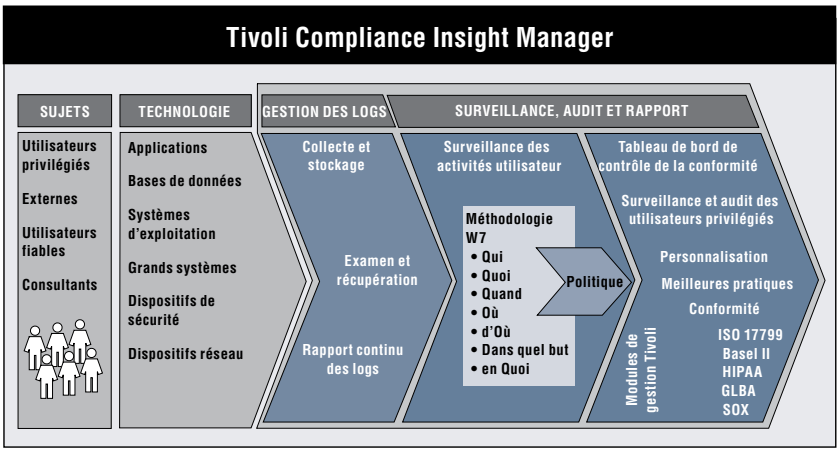
Grâce à sa méthodologie W7, en attente de brevet, Tivoli Compliance Insight Manager convertit les données des logs natifs en langage simple. Alliance performante, la méthodologie W7 et le tableau de bord vous permettent de vérifier rapidement les Qui, Où, Quand, Quoi, d'Où, Dans quel but et en Quoi.

Avec ce type d'informations à portée de main, vous pouvez :

- *Remonter et explorer rapidement les informations relatives au comportement des utilisateurs, à l'activité du système et à la sécurité sur tous les types de plates-formes.*
- *Comparer les entrées des logs à une politique de référence afin d'identifier et de réduire au minimum les problèmes de sécurité.*
- *Fournir des rapports pour répondre aux demandes de justification des auditeurs et aux besoins de contrôle des responsables de la sécurité sans avoir recours à des experts dont les tarifs sont très élevés.*
- *Traiter rapidement les incidents liés à l'activité des utilisateurs grâce à la possibilité de prendre des mesures et de définir des alertes sans entraver le travail des administrateurs.*

Communiquer efficacement les informations d'audit et de conformité et automatiser la distribution des rapports

Capturer et convertir en continu la totalité des données des logs peut simplifier de manière significative la lourde tâche de respecter les mesures de conformité. Tivoli Compliance Insight Manager va plus loin en permettant aux organisations de produire immédiatement des rapports sur les utilisateurs et les données, ainsi que des rapports potentiels personnalisés pour répondre à des besoins particuliers.

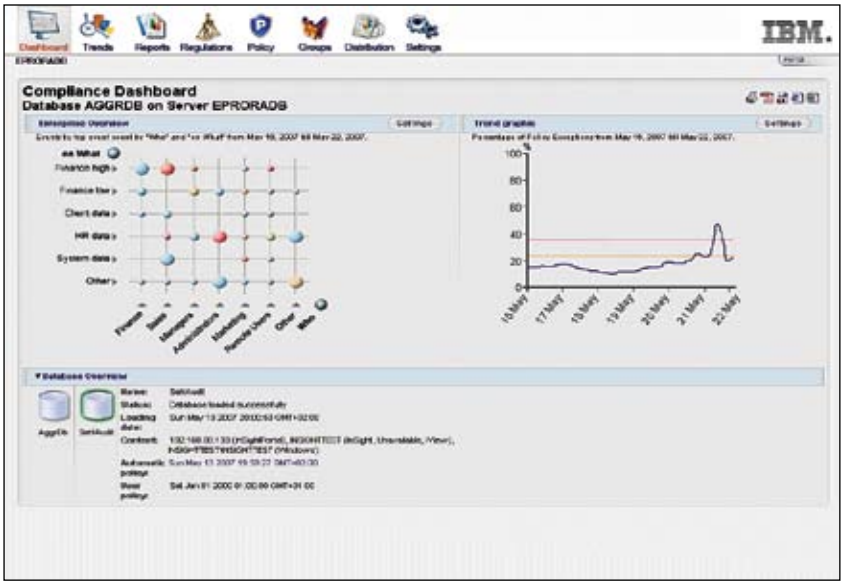


Tivoli Compliance Insight Manager enregistre les informations de sécurité, sur les utilisateurs et au niveau technologique, destinées à la génération de rapports d'audit et de conformité.

Par ailleurs, Tivoli Compliance Insight Manager offre plus de 100 meilleures pratiques, de rapports d'audit et de conformité permettant de satisfaire les exigences en matière de rapports d'audit d'entreprise. Plusieurs modèles – complétés par une politique de référence personnalisable définissant les règles et les groupes de la méthodologie W7 – sont à votre disposition pour vous aider à démarrer le processus de surveillance et de génération de rapports. Le générateur de règles d'administration automatisé vous aide à établir une politique de référence pouvant servir de base aux futures investigations, et vous pouvez personnaliser le système de comparaison par rapport aux règles de sécurité propres à votre organisation.

Grâce au tableau de bord complet, les responsables de la sécurité peuvent immédiatement visualiser le statut de l'organisation en terme de conformité, ce qui leur permet de localiser les problèmes et les éventuelles violations des règles établies qui requièrent un examen et une résolution immédiate.

La fonction de distribution automatisée des rapports vous permet également de définir en toute simplicité les listes de distribution des rapports. Vous pouvez alors envoyer ces rapports aux responsables fonctionnels pour une vérification plus approfondie ou pour toute autre action selon les exigences de vos processus métier internes.



Le tableau de bord Tivoli Compliance Insight Manager vous permet d'obtenir rapidement une vue d'ensemble de votre position par rapport aux exigences de sécurité, de comprendre ce que font les utilisateurs et de surveiller les utilisateurs privilégiés par rapport à des règles de sécurité établies et des systèmes de référence.

Créer des modules personnalisés de gestion de la conformité grâce à des règles d'administration avancées et des moteurs de définition de rapports

La personnalisation des demandes de génération de rapports pour répondre aux besoins spécifiques et détaillés des exigences de conformité et d'audit peut être un processus long et fastidieux. L'outil de génération de rapports automatisé de Tivoli Compliance Insight Manager vous permet d'affiner les besoins de rapports spécifiques de votre organisation. La distribution des rapports que vous créez peut également se faire via la fonction de distribution automatisée permettant leur intégration dans les processus de vérification ou d'autres flux métier.

Capturer les données avec une analyse automatisée des logs d'entreprise

Les logs des événements sont la plupart du temps générés depuis différents endroits dans l'entreprise, et tous doivent être capturés et conservés. L'automatisation et la centralisation de la collecte des logs rendent ce processus plus efficace et permettent de gagner du temps et de l'argent. En effet, Tivoli Compliance Insight Manager vous permet de collecter, de stocker, d'examiner et de récupérer tous les logs d'entreprise de manière fiable et sécurisée à des fins d'investigation et de contrôle du respect de la conformité.

Un collecteur de logs évolutif garantit la collecte, fiable et vérifiable, des logs natifs depuis quasiment toutes les plates-formes. Et tandis que beaucoup de solutions collectent uniquement les logs des protocoles syslog et SNMP (Simple Network Management Protocol), la fonction de gestion des logs de Tivoli Compliance Insight Manager capture presque tous les types de logs de sécurité, notamment :

- *Le coeur des systèmes d'exploitation, dont IBM System z, IBM System i, IBM AIX, Sun Solaris, HP-UX, Microsoft® Windows® et Linux®.*
- *Les traces de contrôle des applications, qu'elles soient écrites dans un fichier ou une table d'une base de données.*
- *Le coeur des bases de données, dont IBM DB2 sur System z, UNIX® et Windows, Oracle Database Server, Microsoft SQL Server et Sybase ACE.*
- *Les logs des dispositifs de sécurité, via Syslog et SNMP.*
- *Les autres produits Tivoli, tels que Tivoli Security Operations Manager, Tivoli Identity Manager et Tivoli Access Manager.*

Afin de pouvoir fournir instantanément aux auditeurs et aux régulateurs des rapports sur la complétude et la continuité de votre programme de gestion et de collecte des logs, Tivoli Compliance Insight Manager offre un rapport continu des logs.

Par ailleurs, grâce à des outils d'analyse optimisés, Tivoli Compliance Insight Manager peut examiner et analyser des incidents suspects via un dépôt de logs condensés longue durée. Ce dépôt dispose de fonctions de recherche conviviales permettant d'identifier les incidents potentiels liés à la sécurité.

Simplifier l'ajout de collecteurs et d'analyseurs

Le kit d'outils avancé de Tivoli Compliance Insight Manager simplifie l'ajout de nouveaux collecteurs et analyseurs. Ces analyseurs peuvent servir à définir des indexeurs permettant d'inclure les données des logs – collectées à partir des fichiers logs n'importe où dans l'entreprise – aux recherches dans l'outil d'investigation du dépôt. Cette fonction vous permet d'effectuer rapidement des analyses couvrant toutes les données des logs en ligne. Vous pouvez ainsi traiter rapidement les incidents sans avoir recours à des outils internes lourds ou à des langages d'analyse très techniques. Une fois les incidents identifiés, il est possible de récupérer les données d'origine pour les utiliser avec des outils légaux supplémentaires ou des outils d'analyse propres aux plates-formes.

Surveiller et contrôler les activités des utilisateurs privilégiés

Au cours des dernières années, les risques liés à la sécurité posés par des sources externes ont fait l'objet d'une attention particulière au niveau des supports. Bien que ces attaques représentent une véritable menace pour les organisations, les incidents de sécurité internes venant des utilisateurs privilégiés représentent une menace encore plus importante. Que ces incidents soient involontaires ou malveillants, leur impact peut aller de l'indisponibilité des activités perdues à la responsabilité légale.

Grâce à Tivoli Compliance Insight Manager, vous pouvez surveiller les activités de ces utilisateurs très puissants afin de vérifier que vos règles établies sont systématiquement respectées – sans ralentir ni entraver leur travail.

Au moment des audits, Tivoli Compliance Insight Manager vous permet de démontrer aux auditeurs que votre organisation :

- *Examine et consigne régulièrement les activités des opérateurs et administrateurs système.*
- *Analyse et examine les incidents liés à la sécurité et les activités suspectes et prend des mesures pour y remédier.*
- *Consigne l'accès aux données sensibles, y compris l'accès de l'administrateur root et de l'administrateur de base de données (DBA).*
- *Gère et vérifie en continu les logs de l'application, de la base de données, du système d'exploitation et des unités.*

Améliorer les fonctions d'audit RACF d'IBM par le biais de plug-ins

Tivoli Compliance Insight Manager comporte en option des plug-ins pour gros systèmes avec des fonctions d'audit RACF avancées, permettant de réduire les coûts et les ressources compétentes nécessaires pour gérer un environnement sécurisé pour vos ressources importantes. Conçus pour répondre à tous les problèmes de conformité et de sécurité propres à la fonction RACF, ces plug-ins permettent aux organisations :

- *D'analyser et de générer rapidement un rapport sur les événements des gros systèmes.*
- *De détecter automatiquement les risques liés à la sécurité grâce à un contrôle étendu des statuts.*
- *De créer des rapports standards et personnalisés pouvant être générés au format XML afin d'être utilisés dans les bases de données et les outils de génération de rapports.*
- *D'identifier rapidement les connexions non autorisées, les utilisateurs violant les règles de sécurité et les systèmes centraux menacés.*
- *De vérifier les commandes RACF par rapport aux règles et procédures de votre société et de bloquer ou corriger celles qui ne sont pas conformes.*

Intégration aux solutions SIEM, de gestion des identités et de contrôle d'accès

Tivoli Compliance Insight Manager vient compléter Tivoli Security Operations Manager pour permettre aux organisations d'améliorer le traitement des incidents et le respect de la conformité aux réglementations. En envoyant les informations sur les événements critiques de Tivoli Compliance Insight Manager à Tivoli Security Operations Manager, le personnel responsable des opérations de sécurité peut prendre des mesures immédiates. Tivoli Security Operations Manager peut également fournir à Tivoli Compliance Insight Manager des données relatives à la violation des réglementations. Par exemple, Tivoli Security Operations Manager peut envoyer à Tivoli Compliance Insight Manager des données particulières si le temps de traitement des incidents dépasse le temps réglementaire de l'entreprise, ce qui permet au personnel responsable de la sécurité d'examiner ces exceptions avant que les mesures de sécurité et de conformité ne soient menacées.

Par ailleurs, Tivoli Compliance Insight Manager s'intègre à Tivoli Identity Manager, IBM Tivoli Access Manager for e-business et à IBM Tivoli Access Manager for Operating Systems. Cela permet de surveiller l'activité administrative sur ces serveurs afin de déterminer si l'activité des administrateurs de Tivoli Identity Manager et de Tivoli Access Manager et les changements qu'ils effectuent respectent votre politique ou les instructions de référence. Tivoli Compliance Insight Manager s'intègre également aux répertoires de l'administrateur de Tivoli Identity Manager et de Tivoli Access Manager de manière à ce que les noms d'utilisateur des utilisateurs de l'administration soient inclus dans les rapports de Tivoli Compliance Insight Manager.

Tivoli Compliance Insight Manager en bref

Configuration minimum requise pour un serveur d'entreprise :

- Processeur 4x Intel® Xeon 3.0 GHz
- RAM : 6 Go
- Windows 2000 Advanced Server SP4 ou Windows 2003 Server SP1
- Microsoft Internet Explorer 6.0 et les versions ultérieures pour l'affichage des rapports HTML

Configuration minimum requise pour un serveur standard :

- Processeur 2x Xeon 3.0 GHz
- RAM : 4 Go
- Windows 2000 Advanced Server SP4 ou Windows 2003 Server SP1
- Microsoft Internet Explorer 6.0 et les versions ultérieures pour l'affichage des rapports HTML
- Syslog-NG 1.6.6 et les versions ultérieures

Les configurations spécifiques seront fonction des volumes des logs et des types de données des logs. Les éléments sus mentionnés représentent les exigences minimum.

Pour en savoir plus

Basée sur une expérience de plus de vingt ans dans les contrôles de la sécurité et la gestion du respect de la conformité, Tivoli Compliance Insight Manager offre une solution phare permettant d'analyser les logs, de surveiller les utilisateurs privilégiés et de générer des rapports d'audit et de conformité dans toute l'entreprise – des systèmes d'exploitation et applications aux bases de données, gros systèmes et unités réseau.

Pour en savoir plus sur les fonctions de Tivoli Compliance Insight Manager permettant à votre organisation de surveiller l'activité des utilisateurs et d'intégrer des travaux de vérification du respect de la conformité, contactez votre représentant ou partenaire commercial IBM, ou rendez-vous sur le site :

ibm.com/tivoli

A propos des logiciels Tivoli d'IBM

La gamme de logiciels Tivoli comporte un ensemble d'offres et de fonctionnalités qui viennent renforcer IBM Service Management, une approche modulaire évolutive établie pour offrir à votre activité des services plus performants. En aidant les entreprises de toute taille à satisfaire leurs besoins, la gamme Tivoli vous permet d'offrir un service d'excellence pour appuyer vos objectifs métier grâce à l'intégration et à l'automatisation des processus, des flux de travaux et des tâches à accomplir. La plate-forme de gestion des services Tivoli, hautement sécurisée et basée sur les standards ouverts, est complétée par des solutions de gestion opérationnelles proactives offrant une visibilité et un système de contrôle complets. Elle est également renforcée par les services et les supports IBM ainsi que par un écosystème proactif de partenaires commerciaux IBM. Les clients et partenaires commerciaux Tivoli peuvent également exploiter les meilleures pratiques de chacun en participant aux groupes d'utilisateurs Tivoli d'IBM (IBM Tivoli User Groups), organisations indépendantes se réunissant un peu partout dans le monde. Pour toute information, rendez-vous sur le site :

www.tivoli-ug.org

Compagnie IBM France
Tour Descartes – La Défense 5
2 avenue Gambetta
92066 – Paris La Défense Cedex
Tel : 0810 011 810
ibm.com/fr

IBM Belgium
Avenue du Bourget/Bourgetlaan, 42
B – 1130 Brussels
ibm.com/be

La page d'accueil d'IBM est accessible sur le site :
ibm.com

Imprimé aux Etats-Unis
06-07

TAKE BACK CONTROL WITH Tivoli®

TID10355-FRFR-00